Bare PAKE: Universally Composable Key Exchange from just Passwords

Manuel Barbosa, Kai Gellert, Julia Hesse*, and Stanislaw Jarecki

University of Porto (FCUP) and INESC TEC and Max Planck Institute for Security and Privacy
mbb@fc.up.pt

University of Wuppertal
kai.gellert@uni-wuppertal.de

IBM Research Europe - Zurich
jhs@zurich.ibm.com

UC Irvine
stanislawjarecki@gmail.com

Abstract. In the past three decades, an impressive body of knowledge has been built around secure and private password authentication. In particular, secure password-authenticated key exchange (PAKE) protocols require only minimal overhead over a classical Diffie-Hellman key exchange. PAKEs are also known to fulfill strong composable security guarantees that capture many password-specific concerns such as password correlations or password mistyping, to name only a few. However, to enjoy both round-optimality and strong security, applications of PAKE protocols must provide *unique* session and participant identifiers. If such identifiers are not readily available, they must be agreed upon at the cost of additional communication flows, a fact which has been met with incomprehension among practitioners, and which hindered the adoption of provably secure password authentication in practice.

In this work, we resolve this issue by proposing a new paradigm for truly *password-only* yet securely composable PAKE, called *bare* PAKE. We formally prove that two prominent PAKE protocols, namely CPace and EKE, can be cast as bare PAKEs and hence do not require pre-agreement of anything else than a password. Our bare PAKE modeling further allows to investigate a novel "reusability" property of PAKEs, i.e., whether n^2 pairwise keys can be exchanged from only n messages, just as the Diffie-Hellman non-interactive key exchange can do in a public-key setting. As a side contribution, this add-on property of bare PAKEs leads us to observe that some previous PAKE constructions relied on unnecessarily strong, "reusable" building blocks. By showing that "non-reusable" tools suffice for standard PAKE, we open a new path towards round-optimal post-quantum secure password-authenticated key exchange.

*The author was supported by the Swiss National Science Foundation (SNSF) under the AMBIZIONE grant "Cryptographic Protocols for Human Authentication and the IoT.